

jm



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,466	04/27/2001	Ian Malcolm Pendlebury	MFL-002	1871

21323 7590 10/26/2004

TESTA, HURWITZ & THIBEAULT, LLP
HIGH STREET TOWER
125 HIGH STREET
BOSTON, MA 02110

EXAMINER

GYORFI, THOMAS A

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 10/26/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/844,466	Applicant(s) PENDLEBURY, IAN MALCOLM	
	Examiner Tom Gyorfi	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-45 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-45 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>6/4/01, 9/16/02</u> . | 6) <input checked="" type="checkbox"/> Other: <u>IDS 3/17/03, IDS 7/7/04</u> . |

1. Claims 1-45 have been examined.

Double Patenting

2. Applicant is advised that should claim 42 be found allowable, claim 43 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. In addition, Applicant is further advised that should claim 44 be found allowable, claim 45 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claim 28 is rejected under 35 U.S.C. 102(b) as being anticipated by Waite et al. (U.S. Patent 5,222,134).

Waite discloses a secure system for activating personal computer software remotely, comprising the act of providing a restricted use application software program (column 3, lines 43-47), establishing communications between the user's computer and

Art Unit: 2135

another computer (column 4, lines 32-36), uploading a fingerprint file containing information uniquely identifying the user from the user's computer to the other computer (column 4, lines 17-22 and lines 32-36), downloading a key file from the other computer to the user's computer (column 5, lines 61-68), and running the application software program on the user's computer (column 6, lines 17-22). Note that it is inherently true of personal computers that the step of loading a program onto a user's computer must necessarily occur between the steps of providing a program and running the program; it can also be argued that loading a program is by itself a means for providing a program.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-6, 8-10, 14, 37, 42, and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hicks et al. (U.S. Patent 5,982,892) and Benson (European Patent EP 0895149), both supplied by Applicant.

Regarding claims 1, 37, 42, and 43, Hicks teaches a system of remote authorization for unlocking data. It comprises the steps of generating an access key [the user key of the Hicks patent] based at least in part on an identifier (Hicks, column 3, lines 23-40), and validating the access key against a user data key [the verification key of the Hicks patent] (Hicks, column 3, lines 63-64 and also column 1, lines 61-64), and

Art Unit: 2135

upon successful validation access to the program is granted (Hicks, column 4, lines 10-14). Hicks does not explicitly teach that the identifier is based on a user file, although it allows for the possibility of some other piece of unique identifying information, which could be construed as a user file (Hicks, column 3, lines 30-33). Nevertheless, Benson teaches a method of protecting a file from unauthorized access, including the step of calculating an identifier from a user file (Benson, page 9, lines 26-27). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to create an identifier for use in the invention disclosed by Hicks that was based at least in part on a user file, in a manner similar to that disclosed by Benson. By including the user data files as part of protected subject matter, this would help prevent unauthorized users from viewing copies of the data (Benson, page 6, lines 21-32).

Further regarding claim 37, it should be noted that the method above is embodied in software components running on a computer system (Hicks, Figure 10B and Benson, page 6, lines 21-22).

Regarding claim 2, note that if the ID and key are invalid, the software prompts the user to enter them, said prompting being an activation routine (Hicks, column 3, lines 65-66).

Regarding claim 3, note that the system disclosed by Hicks protects software from being run by unauthorized users (Hicks, column 1, lines 65-67).

Regarding claim 4, note that a file protected by the system disclosed by Benson serves as input data to a special viewing program (Benson, page 6, lines 21-24 and lines 31-32). Therefore, it would have been obvious to one of ordinary skill in the art at

the time the invention was made to use an input file for a software application as part of the identifier disclosed by Hicks. By including protection information in a user input file as opposed to the protected software itself, this would permit the creation of demonstration files that would allow a user to test the application using only those files that are permitted for use by all, while still restricting the unlimited use of the application to users who are properly authorized to do so.

Regarding claim 5, observe that a CRC checksum is used as part of the identifier (Hicks, column 8, lines 1-25).

Regarding claim 6, Examiner takes Official Notice that all user files include at least one file characteristic, e.g. a file name, file size, timestamp, permissions, etc.

Regarding claim 8, note that the user key generated by the system disclosed by Hicks can contain some other piece of uniquely identifying information (Hicks, column 3, lines 30-34). Although using a file characteristic is not explicitly disclosed, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a characteristic from a file pertinent to the software application being protected as part of the access key. Doing so would help the vendor precisely identify a specific copy of the protected software and correlate it with user ID information for tracking purposes.

Regarding claim 9, note that the user key generated by the system disclosed by Hicks comprises a software application signature (Hicks, column 7, lines 7-14).

Regarding claim 10, note that the user key generated by the system disclosed by Hicks can include a machine ID (Hicks, column 3, lines 30-34), which qualifies as a system characteristic.

Regarding claim 14, note that the system disclosed by Hicks, even as modified by Benson, can store the previously calculated access key and use it for subsequent executions of the software (Hicks, column 4, lines 10-14).

7. Claims 11, 29, 39, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Hicks and Benson as applied to claim 1 above, and further in view of Yuval et al. (U.S. Patent 5,586,186).

Regarding claims 11 and 39, the preferred embodiment of the invention disclosed by Hicks does not include an encryption function for the access key. However, Hicks teaches that it would be beneficial to incorporate the encryption methods found in the Yuval patent as an additional step (Hicks, column 3, lines 7-11). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to make such a modification, for enhanced protection during distribution (Ibid. line 11). Furthermore, claim 39 is additionally rejected based on the grounds cited in claim 1 above.

Regarding claim 29, this claim is an accumulation of the elements of claims 1-2, 4-6, 8-11, and 14. Given that the Hicks disclosure as modified by Benson and Yuval possess each of the recited elements, this claim is rejected based on all the rationales presented in the rejections of the other cited claims, applied cumulatively.

Regarding claim 40, note that if the ID and key are invalid, the software prompts the user to enter them, said prompting being an activation routine (Hicks, column 3, lines 65-66).

8. Claims 12, 13, 31, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hicks and Benson as applied to claims 1 and 29 above, and further in view of Cooper et al. (U.S. Patent 5,757,908).

Regarding claims 12 and 31, neither Hicks nor Benson teaches that the access key has a limited validity lifetime, nor that the lifetime of the access key is determined in part by any particular factor. However, Cooper teaches a method to enable the use of software on a trial basis using a temporary key (Cooper, column 12, lines 17-18). This patent is analogous art as it pertains to protection of software products from unauthorized access. Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was made to establish a limited valid lifetime for the access key found in Hicks as modified by Benson, in a manner similar to that disclosed by Cooper. In so doing, one would gain the ability to permit temporary access to the software product being distributed, allowing the user to try the product before making a decision on whether to purchase it or not.

Regarding claims 13 and 32, note that Cooper teaches that alternate embodiments of that invention allow for a key to expire based either on the elapsed time from the issuance of the key (Cooper, column 12, lines 13-21) or through the use of a counter that iterates the number of access key validations (Cooper, column 12, lines 26-31). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use either criterion as the determining factor for the expiration of the temporary key. By allowing either option, the software vendor gains

the benefit of being able to choose a time-limited or usage-limited restriction on the software, and can set a price for the software accordingly.

9. Claims 15-23, 26, 38, 41, and 44-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Penkava et al. (PCT Patent WO 95/35533) and Benson (European Patent EP 0895149), both supplied by Applicant.

Regarding claims 15, 41, 44, and 45, Penkava discloses a method for preventing the use of software on an unauthorized computer. The system comprises the following features: including an identifier [productprint] in a fingerprint [thumbprint] (Penkava, Figure 12), encrypting said fingerprint (Penkava, page 7, lines 6-9), and associating the fingerprint with the software application as the user data key (Penkava, page 7, lines 9-14). With respect to the latter point, Applicant defines the term "key" [and by extension, "user data key"] in a manner inconsistent with the accepted definition in the art; the user data key as taught by Applicant exists merely as an encoded repository of identifying information that is checked during a validation sequence to determine if access should be granted. Similarly, the thumbprint found in Penkava also exists as an encoded repository of identifying information that is checked during a validation sequence to determine if access should be granted. Further, the thumbprint is associated with the program it protects (Penkava, element 122 of Figure 8, and page 25, lines 14-21).

Penkava is silent regarding the use of an identifier that is based at least in part on a user file. However, Benson teaches a method of protecting a file from unauthorized access. It clearly includes the step of creating an identifier from a user file

(Benson, page 9, lines 26-27). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to create an identifier for use in the invention disclosed by Penkava that was based at least in part on a user file, in a manner similar to that disclosed by Benson. By including the user data files as part of protected subject matter, this would help prevent unauthorized users from viewing copies of the data (Benson, page 6, lines 21-32).

Further regarding claim 38, it should be noted that the method described above is embodied by software components executing on a computer (Penkava, Figure 4, and Benson, page 6, lines 21-22).

Regarding claims 16 and 20, note that a file protected by the system disclosed by Benson serves as input data to a special viewing program (Benson, page 6, lines 21-24 and lines 31-32). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use an input file for a software application as the source for an identifier to be included in the thumbprint required by the invention disclosed by Penkava. By including protection information in a user input file as opposed to the protected software itself, this would permit the creation of demonstration files that would allow a user to test the application using only those files that are permitted for use by all, while still restricting the unlimited use of the application to users who are properly authorized to do so.

Regarding claim 17, note that Penkava teaches the computation of a checksum for the identifier that is based at least in part on a cyclic redundancy check (Penkava, element 225 of Figure 12 and also the entirety of Figure 6).

Regarding claim 18, Examiner takes Official Notice that all user files include at least one file characteristic, e.g. a file name, file size, timestamp, permissions, etc.

Regarding claim 21, note that Penkava teaches that the thumbprint comprises a pre-selected [software application] signature (Penkava, page 7, lines 6-9; and also page 12, line 34 – page 13, line 5).

Regarding claim 22, note that Penkava teaches that the use of system characteristics as part of the authentication process (Penkava, page 15, line 32 – page 16, line 22). Although the details are not explicitly taught to be in the thumbprint, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include them. Doing so would help ensure that the thumbprint would be easily detected if a copy were made to an unauthorized user's machine; the system information contained within would identify it as an unauthorized copy immediately.

Regarding claim 23, note that Benson teaches that a vendor may wait to authorize a customer by sending a keyfile until the vendor receives payment (Benson, page 10, lines 38-43). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to stipulate that, as part of the Penkava disclosure, payment must be made prior to the vendor granting permission to use the software. Since Penkava is silent regarding making payments for using protected software, requiring payment provides an obvious commercial benefit to the vendor.

Regarding claim 26, the software application protected by the method disclosed by Penkava verifies whether a valid thumbprint exists for the software (Penkava, page 13, lines 30-33). It can be understood that the thumbprint is transmitted from the

storage device it was embodied within to the active memory of the software application, using the broadest possible interpretation of the term "transmit".

10. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Penkava and Benson as applied to claim 15 above, and further in view of Waite et al. (U.S. Patent 5,103,476).

In the event that Applicant disputes the rationale put forth in the prior rejection of claim 17 that the checksum found in Penkava is based at least in part on a cyclic redundancy check, then it can be shown to be an obvious development in view of Waite. Waite teaches a secure system for activating personal computer software that includes the step of computing a CRC checksum for user identification and program data to be included in a tamperproof overlay file [fingerprint] (Waite, column 6, lines 46-49). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a CRC checksum as part of the identifier information in the invention disclosed by Penkava as modified by Benson. The use of a CRC checksum helps to ensure that the overlay file [fingerprint] is in fact tamperproof, as any attempt to tamper with it would be easily detected (Waite, column 5, lines 1-15).

11. Claims 24 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Penkava and Benson as applied to claims 23 and 33 above, and further in view of Yuval (U.S. Patent 5,586,186).

Regarding claims 24 and 25, both Penkava and Benson are silent regarding using a credit card to purchase the right to use a vendor's software product. It is Examiner's contention that credit card transactions were well known at the time the invention was made and thus would have been self-evidently obvious to one of ordinary skill in the art to incorporate into the system disclosed by Penkava and Benson as a valid means of paying for software. Nevertheless, there does exist more solid grounds for rejection based on the Yuval disclosure. Yuval teaches an alternate method for controlling unauthorized access to software and information; however, Yuval teaches as prior art that a user could purchase from the vendor, through the use of a credit card, the encryption key needed to access software and information stored on a protected CD-ROM (Yuval, column 1, lines 35-43). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to mandate purchasing the user key via credit card as part of the invention disclosed by Penkava and Benson. Credit cards are well known as an expedient means of conducting commerce, by negating the need to have sufficient cash on hand when making a purchase.

12. Claims 25 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Penkava and Benson as applied to claims 23 and 33 above, and further in view of Jovicic et al. (U.S. Patent 5,855,007).

Regarding claims 25 and 36, both Penkava and Benson are silent regarding using a coupon to purchase the right to use a vendor's software product. It is Examiner's contention that coupon transactions were well known at the time the invention was

made and thus would have been self-evidently obvious to one of ordinary skill in the art to incorporate into the system disclosed by Penkava and Benson as a valid means of paying for software. Nevertheless, there does exist more solid grounds for rejection based on the Jovicic disclosure. Jovicic teaches a system to use electronic coupons to make purchases over the Internet (Jovicic, Abstract). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use coupons as the means for payment of the key in the above combination of Penkava and Benson. It is well known that many customers view coupons as an incentive to buy a particular product; thus, by distributing coupons for the software product one can potentially increase the amount of sales. In the case where the coupon allows for a limited number of uses of the software product or service in question, it would also allow for the customers to try said product or service before deciding on whether to buy it (Jovicic, column 1, lines 10-17).

13. Claims 27 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Penkava and Benson as applied to claim 26 above, and further in view of Hicks.

Regarding claim 27, Although Penkava and Benson are both silent regarding the use of dynamic link libraries as part of the invention, Hicks discloses that the verification key, which corresponds to the user data key of Applicant's claim, can be incorporated into a shared library (Hicks, column 10, lines 38-47). Given that dynamic link libraries are well known in the art as a type of shared library, it would therefore have been obvious to one of ordinary skill in the art at the time the invention was made to store the

Art Unit: 2135

thumbprint [user data key] of the combination of Penkava and Benson in a dynamic link library as taught by Hicks. By making the verification key/thumbprint a separate module, it becomes easier to replace in the event that there is a change in authorization status (a new user, time limit expiration, etc.), without requiring any alteration to the actual program code.

Regarding claim 33, this claim is an accumulation of the elements of claims 15-18, 20-23 and 26-27. Given that the Penkava disclosure as modified by Benson and Hicks possess each of the recited elements, this claim is rejected based on all the rationales presented in the rejections of the other cited claims, applied cumulatively.

14. Claims 7, 19, 30, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over the previously cited references of Hicks, Benson, Penkava and Yuval as applied to claims 1, 15, 29, and 33 above, and further in view of Okada et al. (U.S. Patent 6,144,960).

None of the prior art references cited above teach that a user file that would be used in an access key or fingerprint specifically contains a model name, element count, node count, or match ratio. However, Okada teaches a method to register and manage software, which comprises the step of including a model name in an environment file (Okada, column 3, lines 20-25). This patent is analogous art because it pertains to the endeavor of software authorization. Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was made to allow for at least a model name to be a part of the file that is used for authentication purposes; knowing a model

Art Unit: 2135

name would help the vendor further differentiate among multiple users of the vendor's software product, allowing the vendor to maintain more detailed statistics regarding the protected software product.

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: U.S. Patents 6,792,113; 6,694,434; 6,681,212; 6,651,169; 6,595,856; 6,502,193; 6,343,284; 6,330,549; 6,314,409; 6,105,137; 6,009,525; 5,754,646; 5,671,279; 5,590,197; 5,293,422; and PCT Patent WO99/26123.

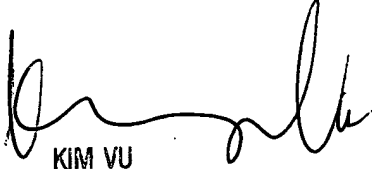
16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:00am - 4:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG
10/20/04



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100